AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Matthew C. Boc being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the United States Drug Enforcement Administration and have been since February of 2012. I have been employed as a Special Agent with the Drug Enforcement Administration ("DEA") since 2012. I am currently assigned to the New England Field Division's Tactical Diversion Squad ("TDS") located in Portsmouth, New Hampshire. Prior to joining DEA's TDS, I was assigned to the Manchester District Office ("MDO") High Intensity Drug Trafficking Area ("HIDTA") Group 2 in Manchester, New Hampshire for approximately four years. Prior to the MDO, I was assigned to the Office of International Training ("TRIB") at Quantico, Virginia for approximately one year. Prior to TRIB, I was assigned to the Foreign-Deployed Advisory and Support Team ("FAST") for approximately six months. Prior to my assignment to FAST, I was assigned to the New York Division Drug Enforcement Task Force ("NYDETF") Group T-31, in New York, New York, for approximately

five years. Prior to my employment as a Special Agent, I was employed as a police officer with the Rye and Dover, New Hampshire Police Departments for approximately nine years.

3. As a DEA Special Agent, I am authorized to investigate violations of the laws of the United States, including violations of federal narcotics laws in Title 21 of the United States Code. I have received training regarding narcotics investigations while attending the Basic Agent Academy in Quantico, Virginia, and have attended additional specialized training courses in furtherance of my past and current assignments.

4. I have participated in all aspects of drug investigations, including physical surveillance, surveillance of undercover transactions, the introduction of undercover agents, the execution of search warrants, the effecting of arrests, and debriefings of defendants, informants and witnesses who had personal knowledge regarding major narcotics trafficking organizations. I have also reviewed recorded conversations and telephone, financial, and drug records. Through my training and experience, I have become familiar with the manner in which illegal drugs are imported, transported, stored, and distributed, and the methods of payment for such drugs. I have also become familiar with the manner in which narcotics organizations utilize various forms of violence and intimidation in furtherance of their narcotics trafficking activity, to protect their operations, members, narcotics, and narcotics proceeds.

5. In my law enforcement training and experience, I have had an opportunity to search for, seize, and personally observe what I have recognized to be and what was later confirmed by drug analysis to be scheduled drugs, including but not limited to heroin, fentanyl, methamphetamine, cocaine, marijuana (both dried and growing), crack cocaine, and various narcotics lawfully available only by prescription. I have conducted or participated in among other things, surveillance, undercover transactions, debriefings of informants and confidential

human sources, and reviews of taped conversations relating to narcotics trafficking. I have assisted in many other investigations, both state and federal. I have drafted drug related search and arrest warrants and have assisted in the execution of numerous search and arrest warrants in which controlled substances, drug paraphernalia, drug related electronic data, and other contraband were found. Through my training and experience, I have become familiar with the habits, methods, routines, practices, and procedures commonly employed by persons engaged in the trafficking of illegal drugs.

6. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I also am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

7. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, information received from other law enforcement officers, including their direct examination of relevant documents, and physical surveillance conducted in connection with persons and places mentioned in this affidavit. The purpose of this affidavit is limited to showing that probable cause exists to support the issuance of a search warrant. Accordingly, while this affidavit contains all the material information, I am aware of that is pertinent to the requested search warrant, it does not include each and every fact known by me or other investigators concerning the investigation.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in **Attachment A** contains evidence related to 21 U.S.C. § 841, 843, and/or 846 as described in Attachment B.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the United States District Court in the District of New Hampshire is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

11. On or about February 2, 2022, DEA Diversion Investigators began an active diversion investigation at a hospital located in Keene, New Hampshire. Due to an internal "self-report" by the hospital, the Keene Police Department was notified that between three hundred to four hundred (300-400) bags of Fentanyl were missing from the hospital and believed to have been stolen. Each bag contained 50 milliliters of a mixture of saline and 2500 micrograms of Fentanyl.

12. On or about February 1, 2022, a nurse at the hospital's Intensive Care Unit ("ICU") went into the Omnicell System (a large vending machine system for medications) to retrieve a 50mL bag of Fentanyl. The bag contains 2500 micrograms of Fentanyl that is diluted in 50mL of saline solution. The Omnicell advised the nurse that the bag had already been removed from the machine by another nurse named Alexandra Towle. Towle was an ICU Nurse

but was not working in the ICU that day. The nurse then went and spoke with Towle about the discrepancy. Towle, who was on duty but not in the ICU that day, denied taking the Fentanyl and explained that there must have been an error within the machine. The following day, Towle was interviewed by Human Resources personnel and her supervisor about the incident. Towle admitted to taking the Fentanyl and left the room to retrieve one of the stolen bags. Towle returned a few minutes later with one of the bags of Fentanyl. Towle was then escorted from the property and suspended indefinitely. An audit was conducted of the inventory of the medications and large discrepancies were found. The audit was able to show that Towle was likely responsible for taking approximately two hundred (200) bags of Fentanyl from the Hospital in the month of January 2022 alone. A further audit determined that Towle had been stealing bags of Fentanyl as far back as August of 2021 for a combine total of over three hundred (300) bags.

13. On February 3, 2022, Keene, New Hampshire Police Detective Donald Lundin spoke with Towle over the phone. Towle agreed to a meeting with Detective Lundin but advised that she wanted to speak with an attorney first. Detective Lundin later spoke with Towle who advised that she had consulted with an attorney who advised her not to speak to law enforcement.

14. On February 4, 2022, Towle contacted a co-worker and close friend at the hospital, a individual I will refer to as "S.M." During that phone call, Towle advised S.M. that she had been suspended from the hospital for stealing the bags of Fentanyl. Towle admitted to S.M. that she had taken over two hundred (200) bags in the month of January 2022. Towle explained that she was addicted to Fentanyl and that she and her fiancé, who I will refer to as "D.G.," were using fentanyl together. Towle then asked S.M. to take more bags of Fentanyl

from the hospital for Towle. S.M. refused Towle's request and later notified her supervision at the hospital.

15. On February 9, 2022, Bureau Chief of Investigations at the Board of Nursing and Pharmacy Certifications Michael Porter contacts Towle over the phone. During the conversation, Towle admitted to stealing the Fentanyl from the hospital. Porter then advised Towle that her Nursing License would be suspended if she did not voluntarily surrender her certification. Towle agreed and signed a document advising that she would not practice nursing until the investigation was completed.

16. On March 3, 2022, Towle committed suicide at her residence in Alstead, New Hampshire. During the course of the death investigation by the Alstead Police Department, the Chief of Police seized Towle's cell phone. The phone was later transferred to the Keene Police Department, at the request of Agents with the DEA.

17. On or about March 4, 2022, D.G., Towle's fiancé left New Hampshire and moved in with his parents in Las Vegas, Nevada.

18. On March 8, 2022, DEA Agents from the Portsmouth Tactical Diversion Squad ("TDS") responded to the Keene Police Department and took custody of Towle's cell phone, a Apple iPhone. Several attempts were made to retrieve the information from Towle's iPhone but all efforts to access the phone were unsuccessful.

19. Later on March 8, 2022, TDS Agents met with DEA Diversion Investigators and retrieved video surveillance footage of Towle taking bags of Fentanyl from the Omnicell at the hospital on a day that she was not scheduled to work. In the video footage, Towle can be seen wearing plain clothes, not hospital scrubs, while taking several Fentanyl bags from the Omnicell

machine. It is uncommon to take as many bags of the Fentanyl as she did for one patient or even several patients.

20. On March 24, 2022, Agents from TDS spoke with S.M. again. S.M. advised that Towle was a very conservative person before she met her fiancé, D.G. S.M. explained that after meeting D.G., Towle's behavior changed drastically. According to S.M., Towle became very liberal with her spending habits and S.M. noticed signs of suspected drug use on both Towle and D.G. S.M. went on to explain that she learned that Goldstein was a recovering drug addict and had recently been enrolled in a rehabilitation facility. S.M. stated that she believed that D.G. had convinced Towle to steal the Fentanyl bags on D.G.'s behalf and that D.G. was distributing the bags through the mail.

21. As of May 2022, none of the stolen bags of Fentanyl have been recovered from Towle, leading me to conclude that they were sent out of the area. Furthermore, the amount of Fentanyl that was stolen is far more than what would typically be considered personal use quantities and therefore, likely could not have been consumed by Towle and D.G. alone.

22. Therefore, there is probable cause to believe that Towle's icloud account contains information regarding the diversion of Fentanyl that Towle admitted to taking from the hospital. It is further believed that the icloud account contains evidence of the diversion of Fentanyl including, but not limited to, images, discussions via text message, and telephone calls to other suspected co-conspirators.

23. Through process served on Apple, we have identified the account described in Attachment A as belonging to Towle. A preservation letter was sent to Apple to preserve the information assigned to Towle's icloud account in April of 2022.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

24. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

25. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be

purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

26. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

27. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

28. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

29. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

30. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

31. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

32. Communications, location services, and financial account information could assist in determining where the stolen Fentanyl was distributed and to whom it was distributed. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

33. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, social media direct messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

34. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. This information will assist in identifying and locating co-conspirators within the drug trafficking organization.

35. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

36. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. Furthermore, Venmo, CashApp and other money remittance apps can assist in identifying co-conspirators within the organization.

37. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

39. Based on the forgoing, I request that the Court issue the proposed search warrant.

40. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

41. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Matthew C. Boc

Matthew C. Boc
Special Agent
United States Drug Enforcement Administration

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: 6/3/22

Time: 1:00 pm

HONORABLE DANIEL J. LYNCH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with Apple iCloud account towle.alexandra@gmail.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California, 95014.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 3, 2022. Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2021 through May 3, 2022, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from January 1, 2021 through May 3, 2022, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 21 U.S.C. § 841, § 843(a)(3), § 843(b) and § 846, since January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Possession with Intent to distribute and distribution of a controlled substance, acquiring controlled substances by misrepresentation, fraud, forgery, deception or subterfuge, use of a communication facility to commit a controlled substance offense, and conspiracy to commit a controlled substance offense.

b. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to Possession with Intent to Distribute a Controlled Substance and Conspiracy to Distribute and Possess with Intent to Distribute a Controlled Substance, including records that help reveal their whereabouts.